MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D. LGS. 8 GIUGNO 2001 N. 231

Approvato dal Consiglio di Amministrazione in data 11.04.2024

Le modifiche rispetto alla revisione precedente sono evidenziate con una barra laterale e riguardano i seguenti paragrafi: 1.2 – 1.3 – 1.5 – 2.1 – 2.7 – 3.4 – 4.1.7

IIS SERVICE srl
Lungobisagno Istria, 15A - 16141 Genova
P.IVA: 01995940994 - Registro Imprese di Genova - REA 451422

INDICE

SEZIONE PRIMA

1. IL DECRETO LEGISLATIVO 8 GIUGNO 2001 N. 231

1.1. LA RESPONSABILITÀ AMMINISTRATIVA DEGLI ENTI

Il D. Lgs. 8 giugno 2001, n. 231, recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica" (di seguito anche il "**D. Lgs. 231/2001**" o **Decreto**), entrato in vigore il 4 luglio 2001 in attuazione dell'art. 11 della Legge Delega 29 settembre 2000 n. 300, ha introdotto nell'ordinamento giuridico italiano, conformemente a quanto previsto in ambito comunitario, la responsabilità amministrativa degli enti, ove per "enti" si intendono le società commerciali, di capitali e di persone, e le associazioni, anche prive di personalità giuridica.

Tale nuova forma di responsabilità, sebbene sia definita "amministrativa" dal legislatore, presenta i caratteri propri della responsabilità penale, essendo rimesso al giudice penale competente l'accertamento dei reati dai quali essa è fatta derivare, ed essendo estese all'ente le medesime garanzie del processo penale.

La responsabilità amministrativa dell'ente deriva dal compimento di reati, espressamente indicati nel D. Lgs. 231/2001, commessi, nell'interesse o a vantaggio dell'ente, da persone fisiche che rivestano funzioni di rappresentanza, amministrazione o direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, o che ne esercitino, anche di fatto, la gestione e il controllo (i cosiddetti "**soggetti apicali**"), ovvero che siano sottoposte alla direzione o vigilanza di uno dei soggetti sopra indicati (i cosiddetti "**sottoposti**").

Oltre all'esistenza dei requisiti sopra descritti, il D. Lgs. 231/2001 richiede anche l'accertamento della colpevolezza dell'ente, al fine di poterne affermare la responsabilità. Tale requisito è riconducibile ad una "colpa di organizzazione", da intendersi quale mancata adozione, da parte dell'ente, di misure preventive adeguate a prevenire la commissione dei reati di cui al successivo paragrafo, da parte dei soggetti espressamente individuati dal Decreto.

Laddove l'ente sia in grado di dimostrare di aver adottato ed efficacemente attuato un'organizzazione idonea ad evitare la commissione di tali reati, attraverso l'adozione del modello di organizzazione, gestione e controllo previsto dal D. Lgs. 231/2001, questi non risponderà a titolo di responsabilità amministrativa.

1.2. I REATI PREVISTI DAL DECRETO

Per il contenuto di questa sezione si rimanda al Modello 231 di IIS Ente Morale (IIS_QSE 017 G rev.2).

1.3. LE SANZIONI COMMINATE DAL DECRETO

Per il contenuto di questa sezione si rimanda al Modello 231 di IIS Ente Morale (IIS_QSE 017 G rev.2).

1.4. CONDIZIONE ESIMENTE DELLA RESPONSABILITÀ AMMINISTRATIVA

Introdotta la disciplina concernente la responsabilità amministrativa dell'ente, l'art. 6 del D. Lgs. 231/2001 stabilisce che lo stesso non risponde a titolo di responsabilità amministrativa, qualora dimostri che:

- l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione, gestione e controllo idonei a prevenire reati della specie di quello verificatosi;
- il compito di vigilare sul funzionamento e l'osservanza dei modelli, e di curarne il relativo aggiornamento, è stato affidato ad un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo (c.d. Organismo di Vigilanza);
- le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione gestione e controllo;
- non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

L'adozione del modello di organizzazione, gestione e controllo, dunque, è condizione necessaria perché l'ente possa sottrarsi all'imputazione di responsabilità amministrativa. La mera adozione di tale documento, con delibera dell'organo amministrativo dell'ente, da individuarsi nel Consiglio di Amministrazione, non è, tuttavia, sufficiente ad escludere *tout court* detta responsabilità, essendo necessario che il modello sia efficacemente attuato da parte dell'ente e dallo stesso effettivamente applicato.

Con riferimento all'efficacia del modello di organizzazione, gestione e controllo per la prevenzione della commissione dei reati previsti dal D. Lgs. 231/2001, si richiede che esso:

- individui, mediante specifica ed esaustiva attività di mappatura dei rischi, le attività nel cui ambito possono essere commessi i reati;

- preveda specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- individui modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- preveda obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
- introduca un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello di organizzazione, gestione e controllo.

Con riferimento all'effettiva applicazione del modello di organizzazione, gestione e controllo, il D. Lgs. 231/2001 richiede:

- un sistema di verifiche sia periodiche sia a sorpresa, e, nel caso in cui siano scoperte significative violazioni delle prescrizioni imposte dal modello o intervengano mutamenti nell'organizzazione o nell'attività dell'ente ovvero modifiche legislative, la modifica del modello di organizzazione, gestione e controllo;
- l'irrogazione di sanzioni in caso di violazione delle prescrizioni imposte dal modello di organizzazione, gestione e controllo, e quindi un sistema disciplinare idoneo a sanzionare il mancato rispetto dello stesso.

1.5. LE "LINEE GUIDA" DI CONFINDUSTRIA

Per il contenuto di questa sezione si rimanda al Modello 231 di IIS Ente Morale (IIS_QSE 017 G rev.2).

SEZIONE SECONDA

2. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI IIS SERVICE

2.1. FINALITÀ DEL MODELLO

IIS SERVICE è società del Gruppo IIS opera in Italia e all'estero, dalla sede centrale di Genova e dagli uffici regionali e/o unità distaccate di Legnano (MI), Mogliano Veneto (TV), Modena (MO), Priolo (SR), Taranto (TA), Roma (RM), Cagliari (CA) e Caserta (CE) e fornisce una vasta gamma di servizi integrati per l'industria, finalizzati ad assicurare l'integrità, l'affidabilità, la disponibilità delle strutture, dei componenti e degli impianti industriali.

Punti di forza di IIS SERVICE sono: l'ingegneria strutturale e di processo, la tecnologia "materials&corrosion", l'ingegneria della saldatura, ed inoltre un'ampia gamma di tecniche di controllo non distruttivo avanzate.

IIS SERVICE vanta anche una lunga esperienza nelle ispezioni, nell'assistenza tecnica in campo e nella sorveglianza in costruzione.

IIS SERVICE ha conseguito la certificazione ISO 9001.

IIS SERVICE ha approvato il presente modello di organizzazione, di gestione e controllo (di seguito anche solo il "**Modello**"), con delibera del Consiglio di Amministrazione del 31.03.2016 e lo ha in seguito aggiornato all'attuale versione con delibera del medesimo CdA in data 11.04.2024.

IIS SERVICE è infatti sensibile all'esigenza di assicurare condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali, a tutela della propria posizione e immagine, e del lavoro dei propri dipendenti ed è, altresì, consapevole dell'importanza di dotarsi di un modello di organizzazione, gestione e controllo (di seguito il "**Modello**"), idoneo a prevenire la commissione di comportamenti illeciti da parte dei propri amministratori, dipendenti e collaboratori sottoposti a direzione o vigilanza da parte della Società.

2.2. DESTINATARI

Le disposizioni del presente Modello sono, dunque, vincolanti per gli amministratori e per tutti coloro che rivestono funzioni di rappresentanza, amministrazione e direzione anche di fatto di IIS SERVICE, per i dipendenti (per tali intendendosi tutti coloro che sono legati a IIS SERVICE da un rapporto di lavoro subordinato, incluso il personale dirigente), per i collaboratori esterni

sottoposti alla direzione o vigilanza del management aziendale di IIS SERVICE (di seguito i "**Destinatari**").

2.3. ELEMENTI FONDAMENTALI DEL MODELLO

Con riferimento alle esigenze individuate nel D. Lgs. 231/2001, gli elementi fondamentali sviluppati da IIS SERVICE nella definizione del Modello, possono essere così riassunti:

- mappatura delle attività sensibili, con esempi di possibili modalità di realizzazione dei reati e dei processi strumentali potenzialmente associabili alla commissione dei reati richiamati dal Decreto, da sottoporre, pertanto, ad analisi e monitoraggio periodico;
- identificazione dei principi etici e delle regole comportamentali volte alla prevenzione di condotte che possano integrare le fattispecie di reato previste dal D. Lgs. 231/2001, sancite nel Codice Etico adottato dal Gruppo IIS, e, più in dettaglio, nel presente Modello;
- previsione di specifici protocolli relativi ai processi strumentali ritenuti a maggior rischio potenziale di commissione di reato, diretti a regolamentare espressamente la formazione e l'attuazione delle decisioni di IIS SERVICE, al fine di fornire indicazioni specifiche sul sistema di controlli preventivi in relazione alle singole fattispecie di illecito da prevenire;
- nomina di un Organismo di Vigilanza collegiale (di seguito anche "**Organismo**" o "**OdV**"), e attribuzione di specifici compiti di vigilanza sull'efficace attuazione ed effettiva applicazione del Modello;
- approvazione di un sistema sanzionatorio idoneo a garantire l'efficace attuazione del Modello, contenente le disposizioni disciplinari applicabili in caso di mancato rispetto delle misure indicate nel Modello medesimo;
- svolgimento di un'attività di informazione e formazione ai Destinatari del presente Modello;
- modalità per l'adozione e l'effettiva applicazione del Modello nonché per le necessarie modifiche o integrazioni dello stesso (aggiornamento del Modello).

2.4. CODICE ETICO E MODELLO

IIS SERVICE, al fine di conformare le proprie attività a principi etici diretti ad improntare le attività aziendali al rispetto delle leggi e regolamenti vigenti in Italia e in tutti i Paesi in cui opera, ha da tempo adottato il proprio Codice Etico del Gruppo IIS, che sancisce i principi di "deontologia aziendale" che IIS SERVICE riconosce come propri.

IIS SERVICE esige l'osservanza dei principi etici contenuti nel Codice Etico da parte di tutti coloro che agiscono in nome e per conto dello stesso e, più in generale, di tutti coloro che, a qualsiasi titolo, entrino in relazione di affari con esso.

Il Codice Etico ha, pertanto, una portata di carattere generale e rappresenta un insieme di regole, adottate spontaneamente da IIS SERVICE, che la stessa riconosce, accetta e condivide, dirette a diffondere una solida integrità etica ed una forte sensibilità al rispetto delle normative vigenti.

Il Modello risponde, invece, a specifiche prescrizioni contenute nel D. Lgs. 231/2001, finalizzate espressamente a prevenire la commissione delle tipologie di reati previste dal Decreto medesimo (per fatti che, apparentemente commessi nell'interesse o a vantaggio dell'ente, possono far sorgere a carico dello stesso una responsabilità amministrativa da reato).

In considerazione del fatto che il Codice Etico richiama principi di comportamento idonei anche a prevenire i reati di cui al D. Lgs. 231/2001, tale documento acquisisce rilevanza ai fini del Modello e costituisce, pertanto, un elemento complementare allo stesso e un valido strumento di prevenzione delle fattispecie penali ricomprese nel Decreto.

2.5. PRESUPPOSTI DEL MODELLO

Il D. Lgs. 231/2001 prevede espressamente, al relativo art. 6, comma 2, lett. a), che il Modello di Organizzazione, Gestione e Controllo dell'ente individui le attività aziendali nel cui ambito possano essere potenzialmente commessi i reati inclusi nel Decreto.

Di conseguenza, IIS SERVICE ha proceduto ad una approfondita analisi delle proprie attività aziendali.

Nell'ambito di tali attività, IIS SERVICE ha, in primo luogo, analizzato la propria struttura organizzativa, rappresentata nell'organigramma aziendale, che individua le Funzioni aziendali, evidenziandone ruoli e linee gerarchiche.

Successivamente, IIS SERVICE ha proceduto alla specifica mappatura dei rischi potenzialmente connessi all'esercizio delle proprie attività aziendali sulla base delle informazioni raccolte dai referenti aziendali (Responsabili di Funzione) che, in ragione del ruolo ricoperto, risultano provvisti della più ampia e profonda conoscenza dell'operatività del settore aziendale di relativa competenza.

I risultati dell'attività sopra descritta sono stati raccolti in una scheda descrittiva (c.d. **Matrice delle Attività a Rischio-Reato**), che illustra in dettaglio i profili di rischio di commissione dei reati richiamati dal D. Lgs. 231/2001, nell'ambito delle attività proprie del Gruppo IIS. Detta Matrice delle Attività a Rischio-Reato è custodita presso la sede di IIS Ente Morale dal Presidente di IIS

SERVICE (Segretario Generale di IIS Ente Morale), che ne cura l'archiviazione, rendendola disponibile per l'eventuale consultazione agli amministratori, ai sindaci, all'Organismo di Vigilanza e a chiunque sia legittimato a prenderne visione.

In particolare, nella Matrice delle Attività a Rischio-Reato vengono rappresentate le aree aziendali a potenziale rischio di commissione dei reati previsti dal D. Lgs. 231/2001 (c.d. "**attività sensibili**"), i reati associabili, gli esempi di possibili modalità a finalità di realizzazione degli stessi, nonché i processi nel cui svolgimento, sempre in linea di principio, potrebbero crearsi le condizioni, gli strumenti e/o i mezzi per la commissione dei reati stessi (c.d. "**processi strumentali**").

Quanto sopra detto, si è ritenuto di redigere il Modello, per IIS SERVICE e per ciascuna delle altre entità del Gruppo, secondo il seguente schema logico-funzionale:

Codice Etico:	Comune all'intero Gruppo IIS;
Modello in "Parte Generale":	Per IIS Ente Morale e per ciascuna delle Società;
Matrice di Rischio:	Comune all'intero Gruppo IIS; in essa, sia le singole attività "a rischio/reato presupposto" (dirette e strumentali) sia l'indicazione degli strumenti a presidio della commissione di reati sono descritte e riferite alla/e singola/e entità (IIS Ente Morale o Società del Gruppo IIS) presso cui sono effettivamente svolte, anche se tali entità sono diverse fra loro. Ritenendo gli estensori del Modello che la separazione di funzioni e attività fra le diverse entità del Gruppo IIS, se correttamente attuata, possa utilmente fungere da presidio contro la commissione di reati/presupposto. Ad. es: il rischio/reato ex art. 2635 comma 3 c.c. (corruzione fra privati) realizzabile mediante l'emissione di falsi certificati sarà indicato come "potenziale" in IIS CERT. Il relativo presidio è invece indicato sia in capo a IIS Ente Morale (struttura del sistema informatico di Gruppo che impedisce ai funzionari tecnici di emettere la documentazione di certificazione) sia in capo a una diversa funzione della stessa IIS CERT (necessità di riesame da parte dell'organo deliberante).

Protocolli di prevenzione: per ciascuna delle entità costituenti il Gruppo IIS sono previsti protocolli (regole organizzative/operative di comportamento) rispetto ai rischi/reato riferibili alla/e singola/ entità.

2.5.1. ATTIVITÀ A RISCHIO-REATO

Nello specifico, è stato riscontrato il rischio di potenziale commissione dei reati previsti dal D. Lgs. 231/2001 nelle seguenti aree di attività aziendale, che vengono di seguito riportate come indicate nella Matrice delle Attività a Rischio-Reato:

A. Rapporti di profilo istituzionale con soggetti appartenenti alla Pubblica Amministrazione;

B. Gestione dei rapporti con gli Enti Pubblici competenti in occasione dell'espletamento degli adempimenti connessi all'attività sociale, anche in occasione di verifiche ed ispezioni;

C. Gestione dell'ideazione, produzione e commercializzazione dei servizi;

D. Gestione dei rapporti con i Clienti ovvero con i fornitori, con particolare riferimento a possibili condotte di corruzione fra privati;

E. Gestione del sistema Sicurezza ai sensi del D. Lgs. 81/08 e successive modifiche ed integrazioni (Testo Unico Sicurezza);

F. Gestione degli adempimenti in materia ambientale;

G. Gestione degli adempimenti richiesti dalla normativa vigente non connessi all'attività caratteristica, anche in occasione di verifiche, ispezioni o accertamenti da parte degli Enti Pubblici competenti e delle Autorità di Vigilanza;

H. Gestione degli adempimenti necessari alla richiesta di finanziamenti e/o agevolazioni e predisposizione della relativa documentazione;

I. Gestione degli adempimenti in materia di assunzioni, cessazione del rapporto di lavoro, retribuzioni, ritenute fiscali e contributi previdenziali e assistenziali, relativi a dipendenti e collaboratori;

J. Gestione dei contenziosi giudiziali e stragiudiziali (es. Civili, tributari, giuslavoristici, amministrativi, penali), in tutti i gradi di giudizio, nomina dei professionisti esterni e coordinamento delle relative attività;

K. Gestione, utilizzo e manutenzione del sistema informativo aziendale;

L. Coordinamento e gestione della contabilità generale, della formazione del bilancio e degli adempimenti tributari e fiscali;

M. Adempimenti societari.

In considerazione delle aree di attività di rischio aziendale sopra riportate sono risultati potenzialmente realizzabili nel contesto aziendale dell'IIS i reati elencati nella Matrice di Rischio.

Il rischio di commissione dei reati non elencati nella Matrice di Rischio, è stato invece ritenuto estremamente remoto in considerazione delle attività svolte dall'IIS e in ogni caso ragionevolmente coperto dal rispetto dei principi etici e delle regole comportamentali enunciate nel Codice Etico adottato dall'IIS, che vincola tutti i suoi destinatari alla più rigorosa osservanza delle leggi e delle normative ad essa applicabili.

2.5.2. PROCESSI STRUMENTALI

Sono stati anche individuati i processi c.d. strumentali nel cui ambito, in linea di principio, potrebbero crearsi le condizioni e/o potrebbero essere forniti gli strumenti per la commissione delle fattispecie di reato:

1. Gestione degli acquisti di beni, servizi e consulenze (ivi compresi gli incarichi professionali);
2. Gestione di donazioni, sponsorizzazioni e omaggi;
3. Selezione, assunzione e gestione del personale dipendente (ivi compresi i rimborsi spese e le spese di rappresentanza);
4. Gestione della produzione e della qualità del prodotto;
5. Gestione delle visite ispettive e dei rapporti con la Pubblica Amministrazione;
6. Gestione della contabilità (e dei flussi finanziari), della formazione del bilancio e rapporti con gli organi sociali;
7. Gestione delle vendite e dei contratti verso clienti pubblici e degli agenti;
8. Gestione degli adempimenti in materia di salute e sicurezza nei luoghi di lavoro;
9. Gestione della sicurezza e manutenzione dei sistemi informativi;
10. Gestione dei finanziamenti pubblici.

2.6. SISTEMA DI CONTROLLO INTERNO

Nella predisposizione del Modello, IIS SERVICE ha tenuto conto del Sistema di Controllo Interno esistente in azienda, al fine di verificare se esso fosse idoneo a prevenire gli specifici reati previsti dal Decreto nelle aree di attività a rischio identificate.

Il sistema di controllo coinvolge ogni settore dell'attività svolta da IIS SERVICE attraverso la distinzione dei compiti operativi da quelli di controllo, riducendo ragionevolmente ogni possibile conflitto di interesse.

In particolare, il sistema di controllo interno di IIS SERVICE si basa, oltre che sulle regole comportamentali previste nel presente Modello, anche sui seguenti elementi:

- il Codice Etico;
- il sistema di protocolli di prevenzione/procedure aziendali;
- la struttura gerarchico-funzionale (organigramma aziendale);
- il sistema di deleghe e procure;
- documenti di governance;
- manuali di gestione.
- sistemi informativi integrati e orientati alla segregazione delle funzioni e alla protezione delle informazioni in essi contenute, con riferimento sia ai sistemi gestionali e contabili che ai sistemi utilizzati a supporto delle attività operative connesse al business.

I principi che regolano le attività nelle aree a rischio e nei processi precedentemente illustrati sono i seguenti:

- esistenza di regole comportamentali di carattere generale a presidio delle attività svolte;
- esistenza e adeguatezza di procedure per la regolamentazione dello svolgimento delle attività nel rispetto dei principi di: tracciabilità degli atti, oggettivazione del processo decisionale e previsione di adeguati punti di controllo;
- rispetto e attuazione concreta del generale principio di separazione dei compiti, secondo cui nessuno deve poter gestire un intero processo in autonomia;
- esistenza di livelli autorizzativi a garanzia di un adeguato controllo del processo decisionale, supportato da un sistema di deleghe e procure riguardante sia i poteri autorizzativi interni, dai quali dipendono i processi decisionali dell'azienda in merito alle operazioni da porre in essere, sia i poteri di rappresentanza per la firma di atti o documenti destinati all'esterno e idonei a vincolare IIS SERVICE nei confronti dei terzi (cosiddette "procure" speciali o generali);
- sistema di comunicazione interna e formazione del personale;
- esistenza di specifiche attività di controllo e di monitoraggio.

La responsabilità, in ordine al corretto funzionamento del sistema dei controlli interni, è rimessa a ciascuna Funzione per tutti i processi di cui essa sia responsabile.

La tipologia di struttura dei controlli aziendali esistente in IIS SERVICE prevede:

- controlli interni di governance, controlli interni del Sistema Integrato Qualità-Sicurezza, controlli interni da parte di soggetti esterni (Organismo di Certificazione ISO 9001).
- controlli di linea, svolti dalle singole Funzioni sui processi di cui hanno la responsabilità gestionale, finalizzati ad assicurare il corretto svolgimento delle operazioni;
- attività di monitoraggio, svolta dai responsabili di ciascun processo e volte a verificare il corretto svolgimento delle attività sottostanti.

Tutto il personale, nell'ambito delle funzioni svolte, è responsabile della definizione e del corretto funzionamento del sistema di controllo, costituito dall'insieme delle attività di verifica che le singole funzioni svolgono sui loro processi.

2.7. REGOLE COMPORTAMENTALI DI CARATTERE GENERALE

Con riferimento alle regole comportamentali di carattere generale che devono essere osservate al fine di prevenire il rischio di commissione dei reati rilevanti ai sensi del Decreto, si rimanda all'apposita Sezione del Modello 231 di IIS Ente Morale (IIS_QSE 017 G rev.2). La violazione di tali regole comporterà l'applicazione delle sanzioni di cui alla sezione quarta.

SEZIONE TERZA

3. ORGANISMO DI VIGILANZA

3.1. PREMESSA

L'art. 6, comma 1, del D. Lgs. 231/2001 prevede che la funzione di vigilare e di curare l'aggiornamento del Modello sia affidata ad un Organismo di Vigilanza interno all'ente che, dotato di autonomi poteri di iniziativa e di controllo, eserciti in via continuativa i compiti ad esso rimessi.

A tale proposito, le Linee Guida di Confindustria evidenziano che, sebbene il D. Lgs. 231/2001 consenta di optare per una composizione sia monocratica che plurisoggettiva, la scelta tra l'una o l'altra soluzione deve tenere conto delle finalità perseguite dalla legge e, quindi, assicurare l'effettività dei controlli in relazione alla dimensione e complessità organizzativa dell'ente.

Non potrà essere nominato componente dell'Organismo di Vigilanza, e, se nominato decade, l'interdetto, l'inabilitato, il fallito o chi è stato condannato, ancorché con condanna non definitiva, ad una pena che importi l'interdizione, anche temporanea, dai pubblici uffici o l'incapacità ad esercitare uffici direttivi ovvero sia stato condannato, anche con sentenza non definitiva o con sentenza di patteggiamento, per aver commesso uno dei reati previsti dal D. Lgs. 231/2001.

Il Decreto richiede, inoltre, che l'Organismo di Vigilanza svolga le sue funzioni al di fuori dei processi operativi dell'Ente, e che sia collocato in posizione di staff al Consiglio di Amministrazione, svincolato da ogni rapporto gerarchico con i singoli responsabili delle funzioni/direzioni aziendali.

In caso di nomina di un componente esterno, lo stesso non dovrà avere rapporti commerciali con IIS SERVICE che possano configurare ipotesi di conflitto di interessi e che possano comprometterne l'indipendenza di giudizio.

In ossequio alle prescrizioni del D. Lgs. 231/2001, alle indicazioni espresse dalle Linee Guida di Confindustria e agli orientamenti della giurisprudenza formatisi in materia, IIS SERVICE ha ritenuto di istituire un organo collegiale, che, per la composizione scelta, possa assicurare autorevolezza, indipendenza e credibilità dello svolgimento delle relative funzioni.

L'Organismo di Vigilanza è stato definito in modo da poter garantire i seguenti requisiti:

- *Autonomia e indipendenza*: detto requisito è assicurato dall'assenza di riporto gerarchico all'interno dell'organizzazione e dalla facoltà di reporting al massimo vertice aziendale.
- *Professionalità*: requisito questo garantito dal bagaglio di conoscenze professionali, tecniche e pratiche, di cui dispongono i componenti dell'Organismo di Vigilanza.
- *Continuità d'azione*: con riferimento a tale requisito, l'Organismo di Vigilanza è tenuto a vigilare costantemente, attraverso poteri di indagine, sul rispetto del Modello, a curarne l'attuazione e l'aggiornamento, rappresentando un riferimento costante per tutto il personale di IIS SERVICE.

L'Organismo di Vigilanza è istituito con l'approvazione del presente Modello. I suoi componenti sono nominati dal Consiglio di Amministrazione secondo le indicazioni del Socio Unico e restano in carica per 3 anni e sono in ogni caso rieleggibili.

Mediante l'approvazione del presente atto sono riconosciuti al suddetto Organismo i poteri e le funzioni di cui ai successivi paragrafi 3.2, 3.3 e 3.4. È inoltre conferito all'Organismo il potere di dotarsi di un proprio regolamento e di approvare uno schema descrittivo dei flussi informativi da e verso di sé.

All'Organismo di Vigilanza è riconosciuto annualmente un budget di spesa adeguato per lo svolgimento delle relative funzioni. L'Organismo delibera in autonomia le spese da sostenere e, in caso di spese eccedenti il budget approvato, dovrà essere autorizzato direttamente dal Consiglio di Amministrazione, sentito il Socio Unico.

La revoca dei membri dell'Organismo di Vigilanza potrà avvenire esclusivamente per giusta causa e previa delibera dell'Socio Unico di IIS SERVICE, sentito il Socio Unico.

3.2. POTERI E FUNZIONI DELL'ORGANISMO DI VIGILANZA

All'Organismo di Vigilanza sono affidati i seguenti compiti:

- vigilare sul funzionamento e osservanza del Modello;
- curarne l'aggiornamento.

Tali compiti sono svolti dall'Organismo attraverso le seguenti attività:

- vigilanza sulla diffusione nel contesto aziendale della conoscenza, della comprensione e dell'osservanza del Modello;
- vigilanza sulla validità ed adeguatezza del Modello, con particolare riferimento ai comportamenti riscontrati nel contesto aziendale;
- verifica dell'effettiva capacità del Modello di prevenire la commissione dei reati previsti dal D. Lgs. 231/2001;
- proposte di aggiornamento del Modello nell'ipotesi in cui si renda necessario e/o opportuno effettuare correzioni e/o adeguamenti dello stesso, in relazione alle mutate condizioni legislative e/o aziendali;
- comunicazione su base continuativa al Consiglio di Amministrazione in ordine alle attività svolte;
- comunicazioni periodiche al Collegio Sindacale/Sindaco Unico su richiesta dello stesso in ordine alle attività svolte;
- occasionalmente nei confronti del Socio Unico e del Collegio Sindacale/Sindaco Unico, nei casi di presunte violazioni poste in essere dai vertici aziendali o dai Consiglieri di Amministrazione, potendo ricevere da detti organi richieste di informazioni o di chiarimenti.

Nello svolgimento di dette attività, l'Organismo provvederà ai seguenti adempimenti:

- istituire specifici canali informativi "dedicati" (indirizzo di posta elettronica dedicato), diretti a facilitare il flusso di segnalazioni ed informazioni verso l'Organismo;
- raccogliere, elaborare, conservare e aggiornare ogni informazione rilevante ai fini della verifica dell'osservanza del Modello;
- verificare e controllare periodicamente le aree/operazioni a rischio individuate nel Modello;
- verificare che le violazioni del Modello siano effettivamente e adeguatamente sanzionate da IIS SERVICE;
- segnalare tempestivamente al Consiglio di Amministrazione, nella persona del Presidente e con i mezzi ritenuti più idonei allo scopo, le presunte violazioni del Modello che abbiano parvenza di fondatezza, laddove le stesse possano coinvolgere la responsabilità di IIS SERVICE in quanto poste in essere da soggetti in posizioni apicali e da dipendenti con qualifica dirigenziale, di cui sia venuto a conoscenza per mezzo di segnalazione o che abbia accertato esso stesso.

Ai fini dello svolgimento degli adempimenti sopra elencati, l'Organismo è dotato dei poteri di seguito indicati:

- accedere liberamente, senza autorizzazioni preventive, a ogni documento aziendale rilevante per lo svolgimento delle funzioni attribuite all'Organismo ai sensi del D. Lgs. 231/2001;
- emanare regolamenti, disposizioni e ordini di servizio intesi a regolare la propria attività;
- disporre che i responsabili delle Funzioni aziendali, e in ogni caso tutti i Destinatari, forniscano tempestivamente le informazioni, i dati e/o le notizie loro richieste per individuare aspetti connessi alle varie attività aziendali rilevanti ai sensi del Modello e per la verifica dell'effettiva attuazione dello stesso da parte delle strutture organizzative aziendali;
- ricorrere a consulenti esterni di comprovata professionalità nei casi in cui ciò si renda necessario per l'espletamento delle attività di verifica e controllo ovvero di aggiornamento del Modello.

Per un miglior svolgimento delle proprie attività, l'Organismo potrà delegare uno o più compiti specifici ai singoli suoi componenti, che li svolgeranno in nome e per conto dell'Organismo stesso. In ordine ai compiti delegati dall'Organismo a singoli membri dello stesso, la responsabilità da essi derivante ricade sull'Organismo nel suo complesso.

3.3. REPORTING DELL'ORGANISMO DI VIGILANZA

Come sopra già anticipato, al fine di garantire la piena autonomia e indipendenza nello svolgimento delle relative funzioni, l'Organismo di Vigilanza comunica direttamente e continuativamente al Consiglio di Amministrazione di IIS SERVICE, e, periodicamente, al Socio Unico ed al Collegio Sindacale/Sindaco Unico.

Il riporto a siffatti organi sociali, costituisce anche la miglior garanzia del controllo ultimo sull'operato degli amministratori, affidato - per previsione legislativa e statutaria - al socio.

Segnatamente, l'Organismo di Vigilanza riferisce a tali organi lo stato di fatto sull'attuazione del Modello, gli esiti dell'attività di vigilanza svolta e gli eventuali interventi opportuni per l'implementazione del Modello:

- in modo continuativo nei confronti del Consiglio di Amministrazione;
- almeno annualmente, al Socio Unico ed al Consiglio di Amministrazione attraverso una relazione scritta nella quale vengono illustrate le attività di monitoraggio svolte, le criticità emerse e gli eventuali interventi correttivi o migliorativi ritenuti opportuni;
- nei confronti del Collegio Sindacale/Sindaco Unico, su richiesta dello stesso in ordine alle attività svolte;
- occasionalmente nei confronti del Socio Unico e del Collegio Sindacale/Sindaco Unico, nei casi di presunte violazioni poste in essere dai vertici aziendali o dai Consiglieri di Amministrazione, potendo ricevere da detti organi richieste di informazioni o di chiarimenti.

L'Organismo di Vigilanza potrà essere convocato in qualsiasi momento e, al contempo, potrà – a sua volta – richiedere al Consiglio di Amministrazione di IIS SERVICE di essere convocato ogni volta che ravveda l'opportunità di un esame o di un intervento in materie inerenti il funzionamento e l'efficace attuazione del Modello o in relazione a situazioni specifiche.

A garanzia di un corretto ed efficace flusso informativo, l'Organismo ha inoltre la possibilità, al fine di un pieno e corretto esercizio dei suoi compiti, di richiedere chiarimenti o informazioni direttamente ai soggetti aventi le principali responsabilità operative.

3.4. FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA E SEGNALAZIONI RILEVANTI EX D.LGS. N. 24/2023

Il D. Lgs. 231/2001 enuncia, tra le esigenze che il Modello deve soddisfare, l'istituzione di obblighi informativi nei confronti dell'Organismo di Vigilanza, diretti a consentire all'Organismo stesso lo

svolgimento delle proprie attività di vigilanza e di verifica sulle aree ritenute dall'Ente a rischio di reato.

A tale proposito devono essere comunicati all'Organismo di Vigilanza le seguenti informazioni:

- su base periodica, le informazioni, dati, notizie e documenti previamente identificati dall'Organismo di Vigilanza secondo le modalità e le tempistiche definite dall'Organismo medesimo;
- su base occasionale, ogni altra informazione, di qualsivoglia natura, attinente l'attuazione del Modello nell'area di attività ritenuta da IIS SERVICE a rischio di reato (c.d. segnalazioni);
- su base occasionale, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del presente decreto e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte.

Sono stati, pertanto, istituiti precisi obblighi gravanti sugli organi sociali e sul personale di IIS SERVICE.

In particolare, gli organi sociali devono riferire all'Organismo di Vigilanza ogni informazione rilevante per il rispetto e il funzionamento del Modello.

I Destinatari devono riferire all'Organismo di Vigilanza ogni informazione relativa a comportamenti che possano integrare violazioni delle prescrizioni del Modello o fattispecie di reato.

Le **segnalazioni (c.d. "whistleblowing")**, invece, potranno avere ad oggetto ogni violazione o sospetto di violazione del Modello od anche ogni altra violazione rilevanti ai sensi del D.Lgs. n. 24/2023.

Ai sensi di tale Decreto Legislativo **ed ai fini del presente Modello231**, si intendono per:

a) «violazioni»: comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'ente e che consistono in una o più delle condotte illecite elencate all'art. 2, comma 1, del D.Lgs. n. 24/2023;

b) «segnalazione» o «segnalare»: la comunicazione scritta od orale di informazioni sulle violazioni;

c) «segnalazione interna»: la comunicazione, scritta od orale, delle informazioni sulle violazioni, presentata tramite il canale di segnalazione interno alla società;

d) «segnalazione esterna»: la comunicazione, scritta od orale, delle informazioni sulle violazioni, presentata tramite il canale di segnalazione esterna di ANAC.

Possono effettuare segnalazioni:

a) i lavoratori subordinati di soggetti del settore privato, ivi compresi i lavoratori il cui rapporto di lavoro è disciplinato dal decreto legislativo 15 giugno 2015, n. 81, o dall'articolo 54-bis del decreto-legge 24 aprile 2017, n. 50, convertito, con modificazioni, dalla legge 21 giugno 2017, n. 96;

b) i lavoratori autonomi, ivi compresi quelli indicati al capo I della legge 22 maggio 2017, n. 81, nonché i titolari di un rapporto di collaborazione di cui all'articolo 409 del codice di procedura civile e all'articolo 2 del decreto legislativo n. 81 del 2015, che svolgono la propria attività lavorativa presso soggetti del settore pubblico o del settore privato;

c) i lavoratori o i collaboratori, che svolgono la propria attività lavorativa presso soggetti del settore pubblico o del settore privato che forniscono beni o servizi o che realizzano opere in favore di terzi;

d) i liberi professionisti e i consulenti che prestano la propria attività presso soggetti del settore pubblico o del settore privato; g) i volontari e i tirocinanti, retribuiti e non retribuiti, che prestano la propria attività presso soggetti del settore pubblico o del settore privato;

e) gli azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto, presso soggetti del settore pubblico o del settore privato.

Incaricato della gestione della segnalazione è un Comitato Etico, che agirà nella massima riservatezza, in modo da garantire i segnalanti contro qualsiasi ritorsione, discriminazione, penalizzazione, assicurando, altresì la segretezza dell'identità del segnalante (salvo la ricorrenza di eventuali obblighi di legge).

In particolare, il sistema di tutela del c.d. *whistleblowing*, come disposto dal D.Lgs. n. 24/2023 è costituito da una piattaforma di segnalazione, raggiungibile dal sito internet della società che consenta, con modalità informatiche, l'invio di segnalazioni con modalità tali da garantire in modo automatico la riservatezza dell'identità del segnalante;

Il Comitato, salvo in caso di segnalazioni anonime che rendano impossibile risalire all'identità del segnalante:

a) dà ricevuta della segnalazione entro sette giorni dalla data di ricezione;

b) mantiene le interlocuzioni con la persona segnalante e può richiedere a quest'ultima, se necessario, integrazioni;

c) dà diligente seguito alle segnalazioni ricevute;

d) fornisce riscontro alla segnalazione entro tre mesi dalla segnalazione;

La società mette a disposizione informazioni chiare sul canale, le procedure ed i presupposti per

effettuare le segnalazioni. Le suddette informazioni sono esposte e rese facilmente visibili nei luoghi di lavoro, nonché pubblicate sul sito internet della società.

Se la persona segnalante ha già effettuato una segnalazione interna e questa non ha avuto seguito, oppure se la persona segnalante ha fondati motivi di ritenere la segnalazione interna possa essere inefficace o esporla a ritorsioni, può allora effettuare una segnalazione esterna tramite il canale attivato sul proprio sito *internet* dall'Autorita' nazionale anticorruzione (ANAC).

Resta fermo il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione. All'uopo, nel sistema disciplinare adottato ai sensi del comma 2, lett. e), sono previste sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.

SEZIONE QUARTA

4. SISTEMA SANZIONATORIO

4.1. DESTINATARI E APPARATO SANZIONATORIO E/O RISOLUTIVO

La definizione di un sistema sanzionatorio, applicabile in caso di violazione delle disposizioni del presente Modello e dei principi del Codice Etico, costituisce condizione necessaria per garantire l'efficace attuazione del Modello stesso, nonché presupposto imprescindibile per consentire a IIS SERVICE di beneficiare dell'esimente dalla responsabilità amministrativa.

L'applicazione delle sanzioni disciplinari prescinde dall'instaurazione e dagli esiti di un procedimento penale eventualmente avviato nei casi in cui la violazione integri un'ipotesi di reato rilevante ai sensi del D. Lgs. 231/2001.

Le sanzioni comminabili sono diversificate in ragione della natura del rapporto tra l'autore della violazione e IIS SERVICE, nonché del rilievo e gravità della violazione commessa e del ruolo e responsabilità dell'autore.

In generale, le violazioni possono essere classificate nei seguenti comportamenti:

- comportamenti che integrano una mancata attuazione colposa delle prescrizioni del Modello, ivi comprese direttive, procedure o istruzioni aziendali;
- comportamenti che integrano una grave trasgressione dolosa delle prescrizioni del Modello, ivi comprese direttive, procedure o istruzioni di IIS SERVICE, tale da compromettere il

rapporto di fiducia tra l'autore e IIS SERVICE in quanto preordinata in modo univoco a commettere un reato.

4.1.1. SANZIONI PER IL PERSONALE DIPENDENTE

In relazione al personale dipendente, IIS SERVICE deve rispettare i limiti di cui all'art. 7 della Legge 300/1970 (c.d. Statuto dei lavoratori) e le previsioni contenute nei contratti vigenti tra IIS SERVICE e i suoi dipendenti (Contratto Collettivo nazionale di lavoro per i dipendenti non dirigenti del Gruppo IIS e Contratto Collettivo Nazionale di Lavoro per i dirigenti di aziende produttrici di beni e servizi), sia con riguardo alle sanzioni comminabili che alle modalità di esercizio del potere disciplinare.

L'inosservanza delle procedure e delle disposizioni indicate nel Modello adottato ai sensi del D. Lgs. 231/2001, nonché le violazioni delle disposizioni e dei principi stabiliti nel Codice Etico da parte del personale dipendente costituisce inadempimento alle obbligazioni derivanti dal rapporto di lavoro ex art. 2104 c.c. e illecito disciplinare.

Più in particolare, l'adozione, da parte di un dipendente di IIS SERVICE, di un comportamento qualificabile, in base a quanto indicato al comma precedente, come illecito disciplinare, costituisce inoltre violazione dell'obbligo dei lavoratori di eseguire con la massima diligenza i compiti loro affidati, attenendosi alle direttive di IIS SERVICE, così come previsto nei contratti vigenti tra IIS SERVICE e i suoi dipendenti (Contratto Collettivo nazionale di lavoro per i dipendenti non dirigenti del Gruppo IIS e Contratto Collettivo Nazionale di Lavoro per i dirigenti di aziende produttrici di beni e servizi).

Con riferimento alle sanzioni irrogabili, esse verranno applicate nel rispetto delle procedure previste dai contratti vigenti applicabili.

Al personale dipendente possono essere comminate le seguenti sanzioni:

- richiamo verbale;
- ammonizione scritta;
- multa;
- sospensione dal lavoro;
- licenziamento.

Tali sanzioni saranno comminate dall'Amministratore Delegato, sulla base del rilievo che assumono le singole fattispecie considerate e saranno proporzionate a seconda della loro gravità.

Al fine di esplicitare preventivamente i criteri di correlazione tra le violazioni dei lavoratori ed i provvedimenti disciplinari adottati, si prevede che:

- Incorre nei provvedimenti disciplinari conservativi il lavoratore che violi le procedure interne o tenga un comportamento non conforme alle prescrizioni del Codice Etico (ad es. che non osservi le procedure prescritte, ometta di dare comunicazione all'Organismo di Vigilanza delle informazioni prescritte, ometta di svolgere controlli, ecc.) o adotti, nell'espletamento di attività nelle aree a rischio, un comportamento non conforme alle prescrizioni contenute nel Modello stesso, dovendosi ravvisare in tali comportamenti una non esecuzione degli ordini impartiti da IIS SERVICE sia in forma scritta che verbale.
- Incorre, inoltre, nei provvedimenti disciplinari risolutivi il lavoratore che:
  - adotti, nell'espletamento delle attività nelle aree a rischio, un comportamento non conforme alle prescrizioni contenute nel Modello e nel Codice Etico, diretto in modo univoco alla commissione di un reato sanzionato dal D. Lgs. 231/2001, dovendosi ravvisare in tale comportamento un'infrazione alla disciplina e alla diligenza nel lavoro, talmente grave da far venire meno la fiducia dell'azienda nei confronti del lavoratore;
  - adotti, nell'espletamento delle attività nelle aree a rischio, un comportamento che si ponga palesemente in contrasto con le prescrizioni contenute nel Modello e nel Codice Etico, tale da determinare la concreta applicazione a carico di IIS SERVICE delle misure previste dal D. Lgs. 231/2001, dovendosi ravvisare in tale comportamento un atto che provoca all'Ente grave nocumento morale e materiale che non consente la prosecuzione del rapporto, neppure in via temporanea.

IIS SERVICE non potrà adottare alcun provvedimento disciplinare nei confronti del dipendente senza avergli preventivamente contestato l'addebito e senza averlo sentito a sua difesa. Salvo che per il richiamo verbale, la contestazione dovrà essere effettuata per iscritto ed i provvedimenti disciplinari non potranno esser comminati prima che siano trascorsi cinque giorni, nel corso dei quali il lavoratore potrà presentare le sue giustificazioni.

Se il provvedimento non verrà comminato entro i sei giorni successivi a tali giustificazioni, queste si riterranno accolte.

Il lavoratore potrà presentare le proprie giustificazioni anche verbalmente, con l'eventuale assistenza di un rappresentante dell'Associazione sindacale cui aderisce.

La comminazione del provvedimento dovrà essere motivata e comunicata per iscritto.

I provvedimenti disciplinari potranno essere impugnati dal lavoratore in sede sindacale, secondo le norme contrattuali relative alle vertenze. Il licenziamento potrà essere impugnato secondo le

procedure previste dall'art. 7 della Legge n. 604 del 15 luglio 1966, confermate dall'articolo 18 della Legge n. 300 del 20 maggio 1970.

Non si terrà conto a nessun effetto dei provvedimenti disciplinari decorsi due anni dalla loro comminazione.

Il tipo e l'entità di ciascuna delle sanzioni sopra elencate saranno determinate in relazione:

- alla gravità della violazione commessa;
- alla mansione, ruolo, responsabilità e autonomia del dipendente;
- alla prevedibilità dell'evento;
- all'intenzionalità del comportamento o grado di negligenza, imprudenza o imperizia;
- al comportamento complessivo dell'autore della violazione, con riguardo alla sussistenza o meno di precedenti disciplinari;
- ad altre particolari circostanze che caratterizzino la violazione.

Le sanzioni disciplinari (così come previsto dall'art. 7 L. 300/70) ed il Codice Etico, sono portate a conoscenza del lavoratore mediante affissione in luogo accessibile a tutti.

4.1.2. SANZIONI PER COLLABORATORI SOTTOPOSTI A DIREZIONE O VIGILANZA

L'inosservanza delle procedure indicate nel Modello adottato da IIS SERVICE ai sensi del D. Lgs. 231/2001, nonché le violazioni delle disposizioni e dei principi stabiliti nel Codice Etico da parte dei collaboratori sottoposti a direzione o vigilanza di IIS SERVICE, potrà determinare, in conformità a quanto disciplinato nello specifico rapporto contrattuale, la risoluzione del relativo contratto, ovvero il diritto di recesso dal medesimo, ferma restando la facoltà di richiedere il risarcimento dei danni verificatisi in conseguenza di detti comportamenti, ivi inclusi i danni causati dall'applicazione da parte del giudice delle misure previste dal D. Lgs. 231/2001.

Tali sanzioni saranno adottate dall'Amministratore Delegato.

4.1.3. SANZIONI PER I LAVORATORI SUBORDINATI CON LA QUALIFICA DI DIRIGENTI

La violazione delle norme di legge, delle disposizioni del Codice Etico e delle prescrizioni previste dal presente Modello commesse da dirigenti, ivi inclusa la violazione degli obblighi di informazione nei confronti dell'Organismo di Vigilanza, nonché, in generale, l'assunzione di comportamenti idonei ad esporre IIS SERVICE all'applicazione di sanzioni amministrative previste dal D. Lgs. 231/2001, potranno determinare l'applicazione delle sanzioni di cui alla contrattazione collettiva per le altre categorie di dipendenti, nel rispetto degli artt. 2106, 2118 e 2119 cod. civ., nonché dell'art. 7 Legge 300/1970.

In via generale, al personale dirigente possono essere comminate le seguenti sanzioni:

- multa;
- sospensione dal lavoro;
- risoluzione anticipata dal rapporto di lavoro.

L'accertamento di eventuali violazioni, nonché dell'inadeguata vigilanza e della mancata tempestiva informazione all'Organismo di Vigilanza, potranno determinare a carico dei lavoratori con qualifica dirigenziale, la sospensione a titolo cautelare dalla prestazione lavorativa, fermo il diritto del dirigente alla retribuzione, nonché, sempre in via provvisoria e cautelare per un periodo non superiore a tre mesi, l'assegnazione ad incarichi diversi nel rispetto dell'art. 2103 cod. civ.

Nei casi di gravi violazioni, IIS SERVICE potrà procedere alla risoluzione anticipata del contratto di lavoro senza preavviso ai sensi e per gli effetti dell'art. 2119 cod. civ.

Tali sanzioni saranno adottate dal Consiglio di Amministrazione.

4.1.4. MISURE NEI CONFRONTI DEGLI AMMINISTRATORI

In caso di violazione accertata del Modello o del Codice Etico da parte degli Amministratori, l'Organismo di Vigilanza informerà tempestivamente l'intero Consiglio di Amministrazione, il Socio Unico e il Collegio Sindacale/Sindaco Unico di IIS SERVICE affinché provvedano ad assumere o promuovere le iniziative più opportune ed adeguate, in relazione alla gravità della violazione rilevata e conformemente ai poteri previsti dalla vigente normativa e dallo Statuto.

In particolare, in caso di violazioni del Modello o del Codice Etico di lieve entità (non diretta in modo univoco ad agevolare o commettere un reato ricompreso nel Decreto) da parte di uno o più Amministratori, il Consiglio di Amministrazione potrà procedere direttamente all'irrogazione della misura sanzionatoria del richiamo formale scritto o della revoca temporanea delle procure.

In caso invece di violazioni del Modello o del Codice Etico da parte di uno o più Amministratori di particolare rilevanza in quanto dirette in modo univoco ad agevolare ovvero a commettere un reato rilevante ai sensi del D. Lgs. 231/2001, le misure sanzionatorie (quali a mero titolo di esempio, la sospensione temporanea dalla carica e, nei casi più gravi, la revoca dalla stessa) saranno adottate dal Socio Unico, sentito il Collegio Sindacale/Sindaco Unico.

4.1.5. MISURE NEI CONFRONTI DEGLI APICALI

In ogni caso, anche la violazione dello specifico obbligo di vigilanza dei sottoposti gravante sugli apicali comporterà, da parte di IIS SERVICE, l'assunzione delle misure sanzionatorie ritenute più opportune in relazione, da una parte, alla natura e gravità della violazione commessa e, dall'altra, alla qualifica del medesimo apicale che dovesse commettere la violazione.

4.1.6. SOGGETTI AVENTI RAPPORTI CONTRATTUALI/COMMERCIALI

La violazione delle disposizioni e dei principi stabiliti nel Codice Etico da parte dei soggetti aventi rapporti contrattuali, commerciali o accordi di partnership con IIS SERVICE, potrà determinare, in conformità a quanto disciplinato nello specifico rapporto contrattuale, la risoluzione del relativo contratto, ovvero il diritto di recesso dal medesimo fermo restando la facoltà di richiedere il risarcimento dei danni verificatisi in conseguenza di detti comportamenti, ivi inclusi i danni causati dall'applicazione da parte del giudice delle misure previste dal D. Lgs. 231/2001.

4.1.7. SANZIONI WHISTLEBLOWING

Il dipendente che violi il divieto di ritorsione nei confronti del segnalante, di cui all'art. 17 del D. Lgs. N. 24/2023 (normativa Whistleblowing) è sanzionato con la sospensione o, nei casi più gravi, con il licenziamento.

L'amministratore che violi il divieto di ritorsione nei confronti del segnalante, di cui all'art. 17 del D. Lgs. N. 24/2023 (normativa Whistleblowing), è sanzionato con la revoca di una o più deleghe, nei casi più gravi, con la revoca della carica.

Il collaboratore esterno che violi il divieto di ritorsione nei confronti del segnalante, di cui all'art. 17 del D. Lgs. N. 24/2023 (normativa Whistleblowing) è sanzionato con la risoluzione del contratto e con la richiesta di risarcimento degli eventuali danni procurati alla Società.

Il precitato art. 17 richiama, senza pretesa di esaustività, alcune fattispecie che, qualora siano riconducibili all'articolo 2, comma 1, lettera m), costituiscono ritorsioni:

a) il licenziamento, la sospensione o misure equivalenti;

b) la retrocessione di grado o la mancata promozione;

c) il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;

d) la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;

e) le note di merito negative o le referenze negative;

f) l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria;

g) la coercizione, l'intimidazione, le molestie o l'ostracismo;

h) la discriminazione o comunque il trattamento sfavorevole;

i) la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione;

l) il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;

m) i danni, anche alla reputazione della persona, in particolare sui social media, o i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi;

n) l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro;

o) la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi;

p) l'annullamento di una licenza o di un permesso;

q) la richiesta di sottoposizione ad accertamenti psichiatrici o medici.

SEZIONE QUINTA

5. INFORMAZIONE E FORMAZIONE DEL PERSONALE

Conformemente a quanto previsto dal D. Lgs. 231/2001, IIS SERVICE ha definito un programma di comunicazione e formazione finalizzato a garantire una corretta divulgazione e conoscenza del Modello e delle regole di condotta in esso contenute, nei confronti delle risorse già presenti in azienda e di quelle da inserire, con differente grado di approfondimento in ragione del diverso livello di coinvolgimento delle stesse nelle attività a rischio.

Il sistema di informazione e formazione è supervisionato ed integrato dall'Organismo di Vigilanza, in collaborazione con la Funzione Risorse Umane e con i responsabili delle Funzioni aziendali di volta in volta coinvolte nell'applicazione del Modello.

In relazione alla comunicazione del Modello, IIS SERVICE si impegna a:

- diffondere il Modello nel contesto aziendale attraverso la pubblicazione sul sito web aziendale e/o con qualsiasi altro strumento ritenuto idoneo;
- predisporre una newsletter destinata a tutto il personale avente qualifica di impiegato, quadro o dirigente;
- organizzare uno specifico incontro formativo nell'ambito del quale illustrare il D. Lgs. 231/2001 ed il Modello adottato.

In ogni caso, l'attività di formazione finalizzata a diffondere la conoscenza della normativa di cui al D. Lgs. 231/2001 e le prescrizioni del Modello adottato sarà differenziata nei contenuti e nelle

modalità in funzione della qualifica dei destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno funzioni di rappresentanza di IIS SERVICE.

Le attività di comunicazione iniziale e di formazione periodica al personale aziendale sarà documentata a cura dell'Organismo di Vigilanza.

SEZIONE SESTA

6. AGGIORNAMENTO DEL MODELLO

L'adozione di eventuali aggiornamenti del Modello compete al Consiglio di Amministrazione, che lo eserciterà mediante delibera con le modalità previste per la sua adozione, sentito previamente il Socio Unico.

L'attività di aggiornamento, intesa sia come integrazione sia come modifica, è volta a garantire l'adeguatezza e l'idoneità del Modello, valutate rispetto alla funzione preventiva di commissione dei reati previsti dal D. Lgs. 231/2001.

Compete, invece, all'Organismo di Vigilanza la concreta verifica circa la necessità od opportunità di procedere all'aggiornamento del Modello, facendosi promotore di tale esigenza nei confronti del Consiglio di Amministrazione e del Socio Unico.